COUNCIL OF THE EUROPEAN UNION

Brussels, 27 November 2013

16987/13

JAI 1078
USA 61
DATAPROTECT 184
COTER 151
ENFOPOL 394

NOTE

from:	Presidency and Commission Services
to:	COREPER
Subject:	Report on the findings by the EU Co-chairs of the ad hoc EU-US Working Group on Data Protection

Delegations will find attached the Report on the findings by the EU Co-chairs of the ad hoc EU-US Working Group on Data Protection.

Report on the findings by the EU Co-chairs of the ad hoc EU-US Working Group on Data Protection

1. AIM AND SETTING UP OF THE WORKING GROUP

In June 2013, the existence of a number of US surveillance programmes involving the large-scale collection and processing of personal data was revealed. The programmes concern in particular the collection of personal data from US internet and telecommunication service providers and the monitoring of data flows inside and outside the US. Given the central position of US information and communications technology companies in the EU market, the transatlantic routing of electronic data flows, and the volume of data flows across the Atlantic, significant numbers of individuals in the EU are potentially affected by the US programmes.

At the EU-US Justice and Home Affairs Ministerial Meeting in June 2013, and in letters to their US counterparts, Vice-President Reding and Commissioner Malmström expressed serious concerns regarding the impact of these programmes on the fundamental rights of individuals in the EU, particularly the fundamental right to protection of personal data. Clarifications were requested from the US authorities on a number of aspects, including the scope of the programmes, the volume of data collected, the existence of judicial and administrative oversight mechanisms and their availability to individuals in the EU, as well as the different levels of protection and procedural safeguards that apply to US and EU persons.

Further to a COREPER meeting of 18 July 2013, an ad hoc EU-US Working Group was established in July 2013 to examine these matters. The purpose was to establish the facts about US surveillance programmes and their impact on fundamental rights in the EU and personal data of EU citizens.

Further to that COREPER meeting, a "second track" was established under which Member States may discuss with the US authorities, in a bilateral format, matters related to their national security, and the EU institutions may raise with the US authorities questions related to the alleged surveillance of EU institutions and diplomatic missions.

On the EU side, the ad hoc Working Group is co-chaired by the Commission and the Presidency of the Council. It is composed of representatives of the Presidency, the Commission services, the European External Action Service, the incoming Presidency, the EU Counter-Terrorism Co-ordinator, the Chair of the Article 29 Working Party, as well as ten experts from Member States, having expertise in the area of data protection and law enforcement/security. On the US side, the group is composed of senior officials from the Department of Justice, the Office of the Director of National Intelligence, the State Department and the Department of Homeland Security.

A preparatory meeting took place in Washington, D.C. on 8 July 2013. Meetings of the Group took place on 22 and 23 July 2013 in Brussels, on 19 and 20 September 2013 in Washington, D.C., and on 6 November 2013 in Brussels.

The findings by the EU co-chairs of the ad hoc EU-US Working Group are presented in this report. The report is based on information provided by the US during the meetings of the ad hoc EU-US working group, as well as on publicly available documents, including classified documents disclosed in the press but not confirmed by the US. Participants on the EU side had an opportunity to submit comments on the report. The US was provided with an opportunity to comment on possible inaccuracies in the draft. The final report has been prepared under the sole responsibility of the EU-co chairs.

The distinction between the EU-US Working Group and the bilateral second track, which reflects the division of competences between the EU and Member States and in particular the fact that national security remains the sole responsibility of each Member State, set some limitations on the discussion in the Working Group and the information provided therein. The scope of the discussions was also limited by operational necessities and the need to protect classified information, particularly information related to sources and methods. The US authorities dedicated substantial time and efforts to responding to the questions asked by the EU side on the legal and oversight framework in which their Signal Intelligence capabilities operate.

2. THE LEGAL FRAMEWORK

The US provided information regarding the legal basis upon which surveillance programmes are based and carried out. The US clarified that the President's authority to collect foreign intelligence outside the US derives directly from his capacity as "commander in chief" and from his competences for the conduct of the foreign policy, as enshrined in the US constitution.

The overall US constitutional framework, as interpreted by the US Supreme Court is also sufficiently relevant to make reference to it here. The protection of the Fourth Amendment of the US Constitution, which prohibits "unreasonable searches and seizures" and requires that a warrant must be based upon "probable cause"[1] extends only to US nationals and citizens of any nation residing within the US. According to the US Supreme Court, foreigners who have not previously developed significant voluntary connections with the US cannot invoke the Fourth Amendment[2].

Two legal authorities that serve as bases for the collection of personal data by US intelligence agencies are: Section 702 of the Foreign Intelligence Surveillance Act of 1978 (FISA) (as amended by the 2008 FISA Amendments Act, 50 U.S.C. § 1881a); and Section 215 of the USA PATRIOT Act 2001 (which also amended FISA, 50 U.S.C. 1861). The FISA Court has a role in authorising and overseeing intelligence collection under both legal authorities.

[1] "Probable cause" must be shown before an arrest or search warrant may be issued. For probable cause to exist there must be sufficient reason based upon known facts to believe a crime has been committed or that certain property is connected with a crime. In most cases, probable cause has to exist prior to arrest, search or seizure, including in cases when law enforcement authorities can make an arrest or search without a warrant.

[2] According to the US Supreme Court, foreigners who are not residing permanently in the US can only rely on the Fourth Amendment if they are part of the US national community or have otherwise developed sufficient connection with the US to be considered part of that community: US v. Verdugo-Urquidez – 494 U.S. 259 (1990), pp. 494 U.S. 264-266.

The US further clarified that not all intelligence collection relies on these provisions of FISA; there are other provisions that may be used for intelligence collection. The Group's attention was also drawn to Executive Order 12333, issued by the US President in 1981 and amended most recently in 2008, which sets out certain powers and functions of the intelligence agencies, including the collection of foreign intelligence information. No judicial oversight is provided for intelligence collection under Executive Order 12333, but activities commenced pursuant to the Order must not violate the US constitution or applicable statutory law.

2.1. Section 702 FISA (50 U.S.C. § 1881a)

2.1.1. Material scope of Section 702 FISA

Section 702 FISA provides a legal basis for the collection of "foreign intelligence information" regarding persons who are "reasonably believed to be located outside the United States." As the provision is directed at the collection of information concerning non-US persons, it is of particular relevance for an assessment of the impact of US surveillance programmes on the protection of personal data of EU citizens.

Under Section 702, information is obtained "from or with the assistance of an electronic communication service provider". This can encompass different forms of personal information (e.g. emails, photographs, audio and video calls and messages, documents and internet browsing history) and collection methods, including wiretaps and other forms of interception of electronically stored data and data in transmission.

The US confirmed that it is under Section 702 that the National Security Agency (NSA) maintains a database known as PRISM. This allows collection of electronically stored data, including content data, by means of directives addressed to the main US internet service providers and technology companies providing online services, including, according to classified documents disclosed in the press but not confirmed by the US, Microsoft, Yahoo, Google, Facebook, PalTalk, AOL, Apple, Skype and YouTube.

The US also confirmed that Section 702 provides the legal basis for so-called "upstream collection"; this is understood to be the interception of Internet communications by the NSA as they transit through the US [1] (e.g. through cables, at transmission points).

Section 702 does not require the government to identify particular targets or give the Foreign Intelligence Surveillance Court (hereafter 'FISC') Court a rationale for individual targeting. Section 702 states that a specific warrant for each target is not necessary.

The US stated that no blanket or bulk collection of data is carried out under Section 702, because collection of data takes place only for a specified foreign intelligence purpose. The actual scope of this limitation remains unclear as the concept of foreign intelligence has only been explained in the abstract terms set out hereafter and it remains unclear for exactly which purposes foreign intelligence is collected. The EU side asked for further specification of what is covered under "foreign intelligence information," within the meaning of FISA 50, U.S.C. §1801(e), such as references to legal authorities or internal guidelines substantiating the scope of foreign intelligence information and any limitations on its interpretation, but the US explained that they could not provide this as to do so would reveal specific operational aspects of intelligence collection programmes. "Foreign intelligence information", as defined by FISA, includes specific categories of information (e.g. international terrorism and international proliferation of weapons of mass destruction) as well as "information relating to the conduct of the foreign affairs of the US." Priorities are identified by the White House and the Director of National Intelligence and a list is drawn up on the basis of these priorities.

Foreign intelligence could, on the face of the provision, include information concerning the political activities of individuals or groups, or activities of government agencies, where such activity could be of interest to the US for its foreign policy[2]. The US noted that "foreign intelligence" includes information gathered with respect to a foreign power or a foreign territory as defined by FISA, 50 USC 1801.

---

1 Opinions of the Foreign Intelligence Surveillance Court (FISC) of 3 October 2011 and of 30 November 2011.

2 50 U.S.C. §1801(e) (2) read in conjunction with §1801(a) (5) and (6).

On the question whether "foreign intelligence information" can include activities that could be relevant to US economic interests, the US stated that it is not conducting any form of industrial espionage and referred to statements of the President of the United States[1] and the Director of National Intelligence[2]. The US explained that it may collect economic intelligence (e.g. the macroeconomic situation in a particular country, disruptive technologies) that has a foreign intelligence value. However, the US underlined that information that is obtained which may provide a competitive advantage to US companies is not authorised to be passed on to those companies.

Section 702 provides that upon issuance of an order by FISC, the Attorney General and the Director of National Intelligence may authorize jointly the targeting of persons reasonably believed to be located outside the US to acquire foreign intelligence information. Section 702 does not require that foreign intelligence information be the sole purpose or even the primary purpose of acquisition, but rather "a significant purpose of the acquisition". There can be other purposes of collection in addition to foreign intelligence. However, the declassified FISC Opinions indicate that, due to the broad method of collection applied under the upstream programme and also due to technical reasons, personal data is collected that may not be relevant to foreign intelligence[3].

---

1 Speaking at a press conference in Stockholm on 4 September 2013, President Obama said: "when it comes to intelligence gathering internationally, our focus is on counterterrorism, weapons of mass destruction, cyber security -- core national security interests of the United States".

2 Statement by Director of National Intelligence James R. Clapper on Allegations of Economic Espionage, 8 September 2013: "What we do not do, as we have said many times, is use our foreign intelligence capabilities to steal the trade secrets of foreign companies on behalf of - or give intelligence we collect to - US companies to enhance their international competitiveness or increase their bottom line"; full statement available at: http://www.dni.gov/index.php/newsroom/press-releases/191-press-releases-2013/926-statement-by-director-of-national-intelligence-james-r-clapper-on-allegations-of-economic-espionage.

3 According to the FISC Declassified Opinion of 3 October 2011, "NSAs 'upstream collection' of Internet communications includes the acquisition of entire 'transactions'", which "may contain data that is wholly unrelated to the tasked selector, including the full content of discrete communications that are not to, from, or about the facility tasked for collection" (p. 5). The FISC further notes that "NSA's upstream collection devices have technological limitations that significantly affect the scope of collection" (p. 30), and that "NSA's upstream Internet collection devices are generally incapable of distinguishing between transactions containing only a single discrete communication to, from, or about a tasked selector and transactions containing multiple discrete communications, not all of which may be to, from or about a tasked selector" (p. 31). It is stated in the FISC Declassified Opinion that "the portions of MCTs [multi communication transactions] that contain references to targeted selectors are likely to contain foreign intelligence information, and that it is not feasible for NSA to limit its collection only to the relevant portion or portions of each MCT" (p. 57).

2.1.2. Personal scope of Section 702 FISA

Section 702 FISA governs the "targeting of persons reasonably believed to be located outside the United States to acquire foreign intelligence information". It is aimed at the targeting of non-US persons who are overseas.

This is confirmed by the limitations set forth in Section 702 (b) FISA which exclusively concern US citizens or non-US persons within the US[1]. More specifically, acquisition of data authorised under Section 702 may not:

(i) intentionally target any person known at the time of acquisition to be located in the US;

(ii) intentionally target a person believed to be located outside the US if the purpose of such acquisition is to target a particular, known person reasonably believed to be in the US;

(iii) intentionally target a US person reasonably believed to be located outside the US;

(iv) intentionally acquire any communication as to which the sender and all intended recipients are known at the time of acquisition to be located in the US.

In addition, pursuant to the same provision, acquisition of data must be "conducted in a manner consistent with the Fourth Amendment to the Constitution of the United States", that prohibits "unreasonable searches and seizures" and requires that a warrant must be based upon "probable cause".

As far as US persons are concerned, the definition of "foreign intelligence information" requires that the information to be collected is *necessary* to the purpose pursued[2]. Concerning non-US persons, the definition of "foreign intelligence information" only requires the information to be *related* to the purpose pursued[3].

---

1 "US person" is defined in 50 U.S.C. §1801(i) as a US citizen, an alien lawfully admitted for permanent residence, an unincorporated association a substantial number of members of which are US citizens or permanent residents, or a corporation incorporated in the US but not including a corporation or association that is a foreign power.

2 50 U.S.C. §1801(e).

3 Ibid.

As discussed below, collection under Section 702 is subject to targeting and minimisation procedures that aim to reduce the collection of personal data of US persons under Section 702, as well as the further processing of personal data of US persons incidentally acquired under Section 702. While, according to the US, non US persons may benefit from some requirements set out in the minimization procedures[1], there are no targeting or minimisation procedures under Section 702 that specifically aim to reduce the collection and further processing of personal data of non-US persons incidentally acquired.

2.1.3. Geographical scope of Section 702 FISA

Section 702 does not contain limitations on the geographical scope of collection of foreign intelligence information.

Section 702 (h) provides that the Attorney General and the Director of National Intelligence may direct an "electronic communication service provider" to provide immediately all information, facilities or assistance necessary. This encompasses a wide range of electronic communication services and operators, including those that may have personal data pertaining to individuals in the EU in their possession:

(i) any service which provides users with the ability to send or receive wire or electronic communications (this could include e.g. email, chat and VOIP providers)[2];

(ii) any "remote computing" service, i.e. one which provides to the public computer storage or processing services by means of an electronic communications system[3];

(iii) any provider of telecommunications services (e.g. Internet service providers)[4]; and

---

1 Declassified minimization procedures (2011) used by the NSA in connection with acquisitions of foreign intelligence information pursuant to Section 702 FISA. See Section 3 (a)

2 FISA s.701 (b)(4)(B); 18 U.S.C. § 2510.

3 FISA s.701 (b) (4) (C); 18 U.S.C. § 2711.

4 FISA s.701 (b) (4) (A); 47 U.S.C. § 153.

(iv) any other communication service provider who has access to wire or electronic communications either as they are transmitted or as they are stored[1].

Declassified FISC opinions confirm that US intelligence agencies have recourse to methods of collection under Section 702 that have a wide reach, such as the PRISM collection of data from internet service providers or through the "upstream collection" of data that transits through the US[2].

The EU asked for specific clarifications on the issue of collection of or access to data not located or not exclusively located in the US; data stored or otherwise processed in the cloud; data processed by subsidiaries of US companies located in the EU; and data from Internet transmission cables outside the US. The US declined to reply on the grounds that the questions pertained to methods of intelligence collection.

2.2. Section 215 US Patriot Act (50 U.S.C. § 1861)

Section 215 of the USA-Patriot Act 2001 is the second legal authority for surveillance programmes that was discussed by the ad hoc EU-US working group. It permits the Federal Bureau of Investigation (FBI) to make an application for a court order requiring a business or another entity to produce "tangible things", such as books, records or documents, where the information sought is relevant for an investigation to obtain foreign intelligence information not concerning a United States person or to protect against international terrorism or clandestine intelligence activities[3]. The order is secret and may not be disclosed. However, the US Office of the Director of National Intelligence declassified and made public some documents related to Section 215, including documents revealing the legal reasoning of the FISC on Section 215.

---

1 FISA s.701 (b) (4) (D).

2 See declassified letters of 4 May 2002 from DOJ and ODNI to the Chairman of the US senate and House of Representatives' Select Committee on Intelligence, p. 3-4 of annexed document.

3 Section 215 further specifies that production of information can relate to an investigation on international terrorism or clandestine intelligence activities concerning a US person, provided that such investigation of a US person is not conducted solely upon the basis of activities protected by the first amendment to the Constitution.

The US confirmed that this provision serves as the basis for a programme of intelligence collection via orders obtained by the FBI from the FISC directing certain telecommunications service providers to provide specified non-content telephony "meta-data". For that programme, the information is stored by the NSA and queried only for counter-terrorism purposes.

That programme is limited to the collection of call detail records, or telephony "meta-data" maintained by specified telecommunications service providers. These records cover information such as telephone numbers dialled and the numbers from which calls are made, as well as the date, time and duration of calls, but do not include the content of the calls, the names, address or financial information of any subscriber or customer, or any cell site location information. According to the explanations provided by the US, this means that the intelligence agencies cannot, through this programme, listen to or record telephone conversations.

The US explained that Section 215 allows for "bulk" collection of telephony meta-data maintained by the company to whom the order is addressed. The US also explained that, although the collection is broad in scope, the further processing of the meta-data acquired under this programme is limited to the purpose of investigation of international terrorism. It was stated that the bulk records may not be accessed or queried by intelligence agencies for any other purpose.

An order for data under Section 215 can concern not only the data of US persons, but also of non-US persons. Both US and EU data subjects, wherever located, fall within the scope of the telephony meta-data programme, whenever they are party to a telephone call made to, from or within the US and whose meta-data is maintained and produced by a company to whom the order is addressed.

There are limitations on the scope of Section 215 generally: when applying for an order, the FBI must specify reasonable grounds to believe that the records sought are relevant to an authorised investigation to obtain foreign intelligence information not concerning a US person, or to protect against international terrorism or clandestine intelligence activities. In addition, US persons benefit under Section 215 from a further protection unavailable to non-US persons, as Section 215 specifically excludes from its scope "investigation of a United States person […] conducted solely upon the basis of activities protected by the first amendment to the Constitution", i.e. activities protected by the freedom of religion, the freedom of speech or of the press, as well as the freedom of assembly and to petition the Government for redress for grievances.

2.3. Executive Order 12333

The US indicated that Executive Order 12333 serves as the basis for other surveillance programmes, the scope of which is at the discretion of the President. The US confirmed that Executive Order 12333 is the general framework on intelligence gathering inside and outside the US. Although the Executive Order requires that agencies operate under guidelines approved by the head of the agency and the Attorney General, the Order itself does not set any restriction to bulk collection of data located outside the US except to reiterate that all intelligence collection must comply with the US Constitution and applicable law. Executive Order 12333 also provides a legal basis to disseminate to foreign governments information acquired pursuant to Section 702[1].

The EU requested further information regarding the scope and functioning of Executive Order 12333 and the guidelines and supplemental procedures whose adoption is provided for under the Executive Order. The EU requested information in particular with regard to the application of Executive Order 12333 to bulk data collection, its impact on individuals in the EU and any applicable safeguards. The US explained that the part that covers signals intelligence annexed to the relevant regulation setting forth procedures under 12333 is classified, as are the supplementary procedures on data analysis, but that the focus of these procedures is on protecting information of US persons. The US indicated that the limitations on intelligence collection under Executive Order 12333 are not designed to limit the collection of personal data of non-US persons. For example, on the question whether collection of inbox displays from email accounts and/or collection of contact lists are authorised, the US representatives replied that they were not aware of a prohibition of such practices.

The US confirmed that judicial approval is not required under Executive Order 12333 and that there is no judicial oversight of its use, except in limited circumstances such as when information is used in a legal proceeding. Executive oversight is exercised under Executive Order 12333 by the Inspector-Generals of each agency, who regularly report to the heads of their agencies and to Congress on the use as well as on breaches of Executive Order 12333. The US was unable to provide any quantitative information with regard to the use or impact on EU citizens of Executive Order 12333. The US did explain, however, that the Executive Order states that intelligence agencies should give "special emphasis" to detecting and countering the threats posed by terrorism, espionage, and the proliferation of weapons of mass destruction[2].

---

1 See Declassified minimization procedures, at p. 11.

2 See Executive Order 12333, Part 1.1 (c).

The US further confirmed that in the US there are other legal bases for intelligence collection where the data of non-US persons may be acquired but did not go into details as to the legal authorities and procedures applicable.

3. COLLECTION AND FURTHER PROCESSING OF DATA

In response to questions from the EU regarding how data is collected and used under the surveillance programmes, the US stated that the collection of personal information based on Section 702 FISA and Section 215 Patriot Act is subject to a number of procedural safeguards and limitative conditions. Under both legal authorities, according to the US, privacy is protected by a multi-layered system of controls on what is collected and on the use of what is collected, and these controls are based on the nature and intrusiveness of the collection.

It appeared from the discussions that there is a significant difference in interpretation between the EU and the US of a fundamental concept relating to the processing of personal data by security agencies. For the EU, data acquisition is synonymous with data collection and is a form of processing of personal data. Data protection rights and obligations are already applicable at that stage. Any subsequent operation carried out on the data collected, such as storage or consultation by human eyes, constitutes further processing. As the US explained, under US law, the initial acquisition of personal data does not always constitute processing of personal data; data is "processed" only when it is analysed by means of human intervention. This means that while certain safeguards arise at that moment of acquisition, additional data protection safeguards arise at the time of processing.

3.1. Section 702 FISA

3.1.1. Certification and authorization procedure

Section 702 does not require individual judicial orders or warrants authorizing collection against each target. Instead, the FISC approves annual certifications submitted in writing by the Attorney General and the Director of National Intelligence. Both the certifications and the FISC's orders are secret, unless declassified under US law. The certifications, which are renewable, identify categories of foreign intelligence information sought to be acquired. They are therefore critical documents for a correct understanding of the scope and reach of collection pursuant to Section 702.

The EU requested, but did not receive, further information regarding how the certifications or categories of foreign intelligence purposes are defined and is therefore not in a position to assess their scope. The US explained that the specific purpose of acquisition is set out in the certification, but was not in a position to provide members of the Group with examples because the certifications are classified. The FISC has jurisdiction to review certifications as well as targeting and minimization procedures. It reviews Section 702 certification to ensure that they contain all required elements and targeting and minimization procedures to ensure that they are consistent with FISA and the Fourth Amendment to the US Constitution. The certification submitted to FISC by the Attorney General and the Director of National Intelligence must contain all the required elements under Section 702 (i), including an attestation that a significant purpose of the acquisition is to obtained foreign intelligence information. The FISC does not scrutinise the substance of the attestation or the need to acquire data against the purpose of the acquisition, e.g. whether it is consistent with the purpose or proportionate, and in this regard cannot substitute the determination made by the Attorney General and the Director of National Intelligence. Section 702 expressly specifies that certifications are not required to identify the specific facilities, places, premises, or property to which an acquisition of data will be directed or in which it will be conducted.

On the basis of FISC-approved certifications, data is collected by means of directives addressed to electronic communications services providers to provide any and all assistance necessary. On the question of whether data is "pushed" by the companies or "pulled" by the NSA directly from their infrastructure, the US explained that the technical modalities depend on the provider and the system they have in place; providers are supplied with a written directive, respond to it and are therefore informed of a request for data. There is no court approval or review of the acquisition of data in each specific case.

According to the US,[1] under Section 702, once communications from specific targets that are assessed to possess, or that are likely to communicate, foreign intelligence information have been acquired, the communications may be queried. This is achieved by tasking selectors that are used by the targeted individual, such as a telephone number or an email address. The US explained that there are no random searches of data collected under Section 702, but only targeted queries. Query terms include names, email addresses, telephone numbers, or keywords. When query terms are used to search databases, there is no requirement of reasonable suspicion neither of unlawful activity nor of a specific investigation. The applicable criterion is that the query terms should be reasonably believed to be used to return foreign intelligence information. The US confirmed that it is possible to perform full-text searches of communications collected, and access both content information and metadata with respect to communications collected.

The targeting decisions made by NSA in order to first acquire communications are reviewed after-the-fact by the Department of Justice and the Office of the Director of National Intelligence; other instances of oversight exist within the executive branch. There is no judicial scrutiny of the selectors tasked, e.g. their reasonableness or their use. The EU requested further information on the criteria on the basis of which selectors are defined and chosen, as well as examples of selectors, but no further clarifications were provided.

[1] See also Semi-Annual Assessment of Compliance with the Procedures and Guidelines Issued Pursuant to Section 702 of the Foreign Intelligence Surveillance Act, Submitted by the Attorney General and the Director of National Intelligence, declassified by the Director of National Intelligence on 21 August 2013 (http://www.dni.gov/files/documents/Semiannual%20Assessment%20of%20Compliance%20with%20procedures%20and%20guidelines%20issued%20pursuant%20to%20Sect%20702%20of%20FISA.pdf), Annex A, p. A2.

The collection of data is subject to specific "minimisation" procedures approved by the FISC. These procedures explicitly apply to information incidentally collected of, or concerning, US persons. They primarily aim to protect the privacy rights of US persons, by limiting the collection, retention, and dissemination of incidentally acquired information to, from or about US persons. There is no obligation to minimize impact on non-US persons outside the US. However, according to the US, the minimisation procedures also benefit non-US persons, since they are aimed at limiting the collection to data reasonably relevant to a foreign intelligence purpose[1]. An example provided by the US in Section 4 of the Minimisation Procedures, which contains attorney-client protections for anyone under indictment in the United States, regardless of citizenship status.

The collection of data is also subject to specific "targeting" procedures that are approved by the FISC. These "targeting" procedures primarily aim to protect the privacy rights of US persons, by ensuring that, in principle, only non-US persons located abroad are targeted. However, the US refers to the fact that the targeting procedures contain factors for the purpose of assessing whether a target possesses and/or is likely to communicate foreign intelligence information[2].

The US did not clarify whether and how other elements of the minimisation and targeting procedures apply in practice to non-US persons, and did not state which rules apply in practice to the collection or processing of non-US personal data when it is not necessary or relevant to foreign intelligence. For example, the EU asked whether information that is not relevant but incidentally acquired by the US is deleted and whether there are guidelines to this end. The US was unable to provide a reply covering all possible scenarios and stated that the retention period would depend on the applicable legal basis and certification approved by FISC.

Finally, the FISC review does not include review of potential measures to protect the personal information of non-US persons outside the US.

---

1 Ibid, at p. 4, Section 3 (b) (4); but see also the declassified November 2011 FISC Opinion which found that measures previously proposed by the government to comply with this requirement had been found to be unsatisfactory in relation to "upstream" collection and processing; and that new measures were only found to be satisfactory for the protection of US persons.

2 See declassified NSA targeting procedures, p 4.

3.1.2. Quantitative indicators

In order to assess the reach of the surveillance programmes under Section 702 and in particular their impact on individuals in the EU, the EU side requested figures, e.g. how many certifications and selectors are currently used, how many of them concern individuals in the EU, or regarding the storage capacities of the surveillance programmes. The US did not discuss the specific number of certification or selectors. Additionally, the US was unable to quantify the number of individuals in the EU affected by the programmes.

The US confirmed that 1.6% of all global internet traffic is "acquired" and 0.025% of it is selected for review; hence 0.0004% of all global internet traffic is looked at by NSA analysts. The vast majority of global internet traffic consists of high-volume streaming and downloads such as television series, films and sports[1]. Communications data makes up a very small part of global internet traffic. The US did not confirm whether these figures included "upstream" data collection.

3.1.3. Retention Periods

The US side explained that "unreviewed data" collected under Section 702 is generally retained for five years, although data collected via upstream collection is retained for two years. The minimisation procedures only state these time limits in relation to US-persons data[2]. However, the US explained that these retention periods apply to all unreviewed data, so they apply to both US and non-US person information.

---

1 See Cisco Visual Networking Index, 2012 (available at: http://www.cisco.com/en/US/solutions/collateral/ns341/ns525/ns537/ns705/ns827/white_paper_c11-481360.pdf)

2 See Declassified minimisation procedures, at p.11, Section 7; and the declassified November 2011 FISC Opinion, at page 13-14: "The two-year period gives NSA substantial time to review its upstream acquisitions for foreign intelligence information but ensures that non-target information that is subject to protection under FISA or the Fourth Amendment [i.e. information pertaining to US persons] is not retained any longer than is reasonably necessary... the Court concludes that the amended NSA minimization procedures, as NSA is applying them to ["upstream collection" of Internet transactions containing multiple communications], are "reasonably designed ... to minimize the ... retention[] ... of non-publicly available information concerning unconsenting United States persons consistent with the need of the United States to obtain, produce, and disseminate foreign intelligence information."

If the data is deemed to be of foreign intelligence interest, there is no limitation on the length of retention. The US did not specify the retention period of data collected under Executive Order 12333.

The EU asked what happens to "non-responsive" information (i.e. data collected that does not respond to query on the basis of a query term). The US responded that it is not "collecting" non-responsive information. According to the US, information that is not reviewed pursuant to a query made to that database normally will "age off of the system". It remains unclear whether and when such data is deleted.

3.1.4. Onward transfers and sharing of information

The US indicated that the collected data are stored in a secure database with limited access for authorised staff only. The US however also confirmed that in case data collected under Section 702 reveal indications of criminal conduct, they can be transferred to or shared with other agencies outside the intelligence community, e.g. law enforcement agencies, for purposes other than foreign intelligence and with third countries. The minimisation procedures of the recipient agency are applicable. "Incidentally obtained" information (information not relevant to foreign intelligence) may also be shared if such information meets the standard under the applicable procedures.
On the use of private contractors, the US insisted that all contractors are vetted and subject to the same rules as employees.

3.1.5. Effectiveness and added value

The US stated that in 54 instances, collection under Sections 702 and 215 contributed to the prevention and combating of terrorism; 25 of these involved EU Member States. The US was unable to provide figures regarding Executive Order 12333. The US confirmed that out of the total of 54 cases, 42 cases concerned plots that were foiled or disrupted and 12 cases concerned material support for terrorism cases.

3.1.6. Transparency and remedies ex-post

The EU asked whether people who are subject to surveillance are informed afterwards, where such surveillance turns out to be unjustified. The US stated that such a right does not exist under US law. However, if information obtained through surveillance programmes is subsequently used for the purposes of criminal proceedings, the protections available under US criminal procedural law apply.

3.1.7. Overarching limits on strategic surveillance of data flows

The EU asked whether surveillance of communications of people with no identified link to serious crime or matters of state security is limited, for example in terms of quantitative limits on the percentage of communications that can be subject to surveillance. The US stated that no such limits exist under US law.

3.2. Section 215 US Patriot Act

3.2.1. Authorization procedure

Under the Section 215 programme discussed herein, the FBI obtains orders from the FISC directing telecommunications service providers to provide telephony meta-data. The US explained that, generally, the application for an order from the FISC pursuant to Section 215 must specify reasonable grounds to believe that the records are relevant to an authorised investigation to obtain foreign intelligence information not concerning a US person or to protect against international terrorism or clandestine intelligence activities. Under the telephony metadata collection programme, the NSA, in turn, stores and analyses these bulk records which can be queried only for counterterrorism purposes. The US explained that the information sought must be "relevant" to an investigation and that this is understood broadly, since a piece of information that might not be relevant at the time of acquisition could subsequently prove to be relevant for an investigation. The standard applied is less stringent than "probable cause" under criminal law and permits broad collection of data in order to allow the intelligence authorities to extract relevant information.

The legal standard of relevance under Section 215 is interpreted as not requiring a separate showing that every individual record in the database is relevant to the investigation. It appears that the standard of relevance is met if the entire database is considered relevant for the purposes sought.[1] While FISC authorization is not required prior to the searching of the data by the NSA, the US stated that Court has approved the procedures governing access to the meta-data acquired and stored under the telephony meta-data programme authorised under Section 215. A small number of senior NSA officials have been authorised to determine whether the search of the database meets the applicable legal standard. Specifically, there must be a "reasonable, articulable suspicion" that an identifier (e.g. a telephone number) used to query the meta-data is associated with a specific foreign terrorist organisation. It was explained by the US that the "reasonable, articulable suspicion" standard constitutes a safeguard against the indiscriminate querying of the collected data and greatly limits the volume of data actually queried.

The US also stressed that they consider that constitutional privacy protections do not apply to the type of data collected under the telephony meta-data programme. The US referred to case-law of the US Supreme Court[2] according to which parties to telephone calls have no reasonable expectation of privacy for purposes of the Fourth Amendment regarding the telephone numbers used to make and receive calls; therefore, the collection of meta-data under Section 215 does not affect the constitutional protection of privacy of US persons under the Fourth Amendment.

3.2.2. Quantitative indicators

The US explained that only a very small fraction of the telephony meta-data collected and retained under the Section 215-authorised programme is further reviewed, because the vast majority of the data will never be responsive to a terrorism-related query. It was further explained that in 2012 less than 300 unique identifiers were approved as meeting the "reasonable, articulable suspicion" standard and were queried. According to the US, the same identifier can be queried more than once, can generate multiple responsive records, and can be used to obtain second and third-tier contacts of the identifier (known as "hops"). The actual number of queries can be higher than 300 because multiple queries may be performed using the same identifier. The number of persons affected by searches on the basis of these identifiers, up to third-tier contacts, remains therefore unclear.

---

1 See letter from DOJ to Representative Sensenbrenner of 16 July 2013 (http://beta.congress.gov/congressional-record/2013/7/24/senate-section/article/H5002-1)

2 U.S. Supreme Court, *Smith v. Maryland*, 442 U.S. 735 (1979):

In response to the question of the quantitative impact of the Section 215 telephony meta-data programme in the EU, for example how many EU telephone numbers calling into the US or having been called from the US have been stored under Section 215-authorised programmes, the US explained that it was not able to provide such clarifications because it does not keep this type of statistical information for either US or non-US persons.

3.2.3. Retention periods

The US explained that, in principle, data collected under Section 215 is retained for five years, with the exception for data that are responsive to authorized queries. In regard to data that are responsive to authorized queries, the data may be retained pursuant to the procedures of the agency holding the information, e.g. the NSA or another agency such as the FBI with whom NSA shared the data. The US referred the Group to the "Attorney General's Guidelines for Domestic FBI Operations"[1] which apply to data that is further processed in a specific investigation. These Guidelines do not specify retention periods but provide that information obtained will be kept in accordance with a records retention plan approved by the National Archives and Records Administration. The National Archives and Records Administration's General Records Schedules do not establish specific retention periods that would be appropriate to all applications. Instead, it is provided that electronic records should be deleted or destroyed when "the agency determines they are no longer needed for administrative, legal, audit or other operational purposes".[2] It follows that the retention period for data processed in a specific investigation is determined by the agency holding the information or conducting the investigation.

[1] Available at: http://www.justice.gov/ag/readingroom/guidelines.pdf, p. 35.

[2] Available at: http://www.archives.gov/records-mgmt/grs/grs20.html: "The records covered by several items in this schedule are authorized for erasure or deletion when the agency determines that they are no longer needed for administrative, legal, audit, or other operational purposes. NARA cannot establish a more specific retention that would be appropriate in all applications. Each agency should, when appropriate, determine a more specific disposition instruction, such as "Delete after X update cycles" or "Delete when X years old," for inclusion in its records disposition directives or manual. NARA approval is not needed to set retention periods for records in the GRS that are authorized for destruction when no longer needed."

3.2.4. Onward transfers and sharing of information

The EU asked for details with regards to sharing of data collected under Section 215 between different agencies and for different purposes. According to the US, the orders for the production of telephony meta-data, among other requirements, prohibit the sharing of the raw data and permit NSA to share with other agencies only data that are responsive to authorized queries for counterterrorism queries. In regard to the FBI's handling of data that it may receive from the NSA, the US referred to the "Attorney General's Guidelines for Domestic FBI Operations"[1]. Under these guidelines, the FBI may disseminate collected personal information to other US intelligence agencies as well as to law enforcement authorities of the executive branch (e.g. Department of Justice) for a number of reasons or on the basis of other statutes and legal authorities[2].

4. OVERSIGHT AND REDRESS MECHANISMS

The US explained that activities authorised by Section 702 FISA and Section 215 Patriot Act are subject to oversight by the executive, legislative and judicial branches.

The oversight regime and the balance between the roles of each of the branches in overseeing the surveillance programmes differ according to the legal basis of collection. For instance, because judicial oversight is limited in relation to Section 702 and collection under Executive Order 12333 is not subject to judicial oversight, a greater role is played by the executive branch in these cases. Oversight regarding whether collection on a foreign target is in keeping with Section 702 would appear to take place largely with the Department of Justice and the Office of the Director of National Intelligence as the responsible departments of the executive branch.

---

1 Available at: http://www.justice.gov/ag/readingroom/guidelines.pdf.

2 Attorney General's Guidelines for Domestic FBI Operations, p. 35-36, provide that "[t]he FBI shall share and disseminate information as required by statutes, treaties, Executive Orders, Presidential directives, National Security Council directives, Homeland Security Council directives, and Attorney General-approved policies, memoranda of understanding, or agreements".

4.1. Executive oversight

Executive Branch oversight plays a role both prior to the collection of intelligence and following the collection, with regard to the processing of the intelligence. The National Security Division of the Department of Justice oversees the implementation of its decisions on behalf of the US intelligence community. These attorneys, together with personnel from the Office of the Director of National Intelligence, review each tasking under FISA 702 (checking justification for a valid foreign intelligence purpose; addressing over-collection issues, ensuring that incidents are reported to the FISC) and the request for production under Section 215 Patriot Act. The Department of Justice and the Office of the Director of National Intelligence also submit reports to Congress on a twice-yearly basis and participates in regular briefings to the intelligence committees of both the House of Representatives and the Senate to discuss FISA-related matters.

Once the data is collected, a number of executive oversight mechanisms and reporting procedures apply. There are internal audits and oversight controls (e.g. the NSA employs more than 300 personnel who support compliance efforts). Each of the 17 agencies that form the intelligence community, including the Office of the Director of National Intelligence has a General Counsel and an Inspector General. The independence of certain Inspectors General is protected by a statute and who can review the operation of the programmes, compel the production of documents, carry out on-site inspections and address Congress when needed. Regular reporting is done by the executive branch and submitted to the FISC and Congress.

As an example, the NSA Inspector-General in a letter of September 2013 to Congress referred to twelve compliance incidents related to surveillance under Executive Order 12333.In this context, the US drew the Group's attention to the fact that since 1 January 2003 nine individuals have been investigated in relation to the acquisition of data related to non-US persons for personal interests. The US explained that these employees either retired, resigned or were disciplined.

There are also layers of external oversight within the Executive Branch by the Department of Justice, the Director of National Intelligence and the Privacy and Civil Liberties Oversight Board.

The Director of National Intelligence plays an important role in the definition of the priorities which the intelligence agencies must comply with. The Director of National Intelligence also has a Civil Liberties Protection Officer who reports directly to the Director.

The Privacy and Civil Liberties Oversight Board was established after 9/11. It is comprised of four part-time members and a full-time chairman. It has a mandate to review the action of the executive branch in matters of counterterrorism and to ensure that civil liberties are properly balanced. It has investigation powers, including the ability to access classified information.

While the US side provided a detailed description of the oversight architecture,[1] the US did not provide qualitative information on the depth and intensity of oversight or answers to all questions about how such mechanisms apply to non-US persons.

4.2. Congressional oversight

Congressional oversight of intelligence activities is conducted through the Intelligence Committee and the Judiciary Committee of both Senate and the House, which employ approximately 30 to 40 staff. The US emphasised that both Committees are briefed on a regular basis, including on significant FISC opinions authorising intelligence collection programmes, and that there was specific re-authorisation of the applicable laws by Congress, including the bulk collection under Section 215 Patriot Act [2].

4.3. Judicial oversight: FISC role and limitations

The FISC, comprised of eleven Federal judges, oversees intelligence activities that take place on the basis of Section 702 FISA and Section 215 Patriot Act. Its proceedings are *in camera* and its orders and opinions are classified, unless they are declassified. The FISC is presented with government requests for surveillance in the form of authorisations for collection or certifications, which can be approved, sent back for improvement, e.g. to be modified or narrowed down, or refused. The number of formal refusals is very small. The US explained that the reason for this is the amount of scrutiny of these requests by different layers of administrative control before reaching the FISC, as well as the iterative process between the FISC and the administration prior to a FISC decision. According to the US, FISC has estimated that at times approximately 25% of applications submitted are returned for supplementation or modification.

---

1 See Semi-Annual Assessment of Compliance.

2 In addition, the Congressional committees are provided with information from the FISC regarding its procedures and working methods; see, for example, the letters of FISA Court Presiding Judge Reggie Walton to Senator Leahy of 29 July 2013 and 11 October 2013.

What exactly is subject to judicial oversight depends on the legal basis of collection. Under Section 215, the Court is asked to approve collection in the form of an order to a specified company for production of records. Under Section 702, it is the Attorney General and the Director of National Intelligence that authorise collection, and the Court's role consists of confirmation that the certifications submitted contain all the elements required and that the procedures are consistent with the statute. There is no judicial oversight of programmes conducted under Executive Order 12333.

The limited information available to the Working Group did not allow it to assess the scope and depth of oversight regarding the impact on individuals in the EU. As the limitations on collection and processing apply primarily to US persons as required by the US Constitution, it appears that judicial oversight is limited as far as the collection and further processing of the personal data of non-US persons are concerned.

Under Section 702, the FISC does not approve government-issued directives addressed to companies to assist the government in data collection, but the companies can nevertheless bring a challenge to a directive in the FISC. A decision of the FISC to modify, set aside or enforce a directive can be appealed before the FISA Court of Review. Companies may contest directives on grounds of procedure or practical effects (e.g. disproportionate burden or departure from previous orders). It is not possible for a company to mount a challenge on the substance as the reasoning of the request is not provided.

FISC proceedings are non-adversarial and there is no representation before the Court of the interests of the data subject during the consideration of an application for an order. In addition, the US Supreme Court has established that individuals or organisations do not have standing to bring a lawsuit under Section 702, because they cannot know whether they have been subject to surveillance or not[1]. This reasoning would apply to both US and EU data subjects. In light of the above, it appears that individuals have no avenues for judicial redress under Section 702 of FISA.

[1] *Clapper v Amnesty International*, Judgment of 26 February 2013, 568 U. S. (2013)

5. SUMMARY OF MAIN FINDINGS

(1) Under US law, a number of legal bases allow large-scale collection and processing, for foreign intelligence purposes, including counter-terrorism, of personal data that has been transferred to the US or is processed by US companies. The US has confirmed the existence and the main elements of certain aspects of these programmes, under which data collection and processing is done with a basis in US law that lays down specific conditions and safeguards. Other elements remain unclear, including the number of EU citizens affected by these surveillance programmes and the geographical scope of surveillance programmes under Section 702.

(2) There are differences in the safeguards applicable to EU data subjects compared to US data subjects, namely:

i. Collection of data pertaining to US persons is, in principle, not authorised under Section 702. Where it is authorised, data of US persons is considered to be "foreign intelligence" only if *necessary* to the specified purpose. This necessity requirement does not apply to data of EU citizens which is considered to be "foreign intelligence" if it *relates* to the purposes pursued. This results in lower threshold being applied for the collection of personal data of EU citizens.

ii. The targeting and minimisation procedures approved by FISC under Section 702 are aimed at reducing the collection, retention and dissemination of personal data of or concerning US persons. These procedures do not impose specific requirements or restrictions with regard to the collection, processing or retention of personal data of individuals in the EU, even when they have no connection with terrorism, crime or any other unlawful or dangerous activity. Oversight of the surveillance programmes aims primarily at protecting US persons.

iii. Under both Section 215 and Section 702, US persons benefit from constitutional protections (respectively, First and Fourth Amendments) that do not apply to EU citizens not residing in the US.

(3) Moreover, under US surveillance programmes, different levels of data protection safeguards apply to different types of data (meta-data vs. content data) and different stages of data processing (initial acquisition vs. further processing/analysis).

(4) A lack of clarity remains as to the use of other available legal bases, the existence of other surveillance programmes as well as limitative conditions applicable to these programmes. This is especially relevant regarding Executive Order 12333.

(5) Since the orders of the FISC are classified and companies are required to maintain secrecy with regard to the assistance they are required to provide, there are no avenues, judicial or administrative, for either EU or US data subjects to be informed of whether their personal data is being collected or further processed. There are no opportunities for individuals to obtain access, rectification or erasure of data, or administrative or judicial redress.

(6) Various layers of oversight by the three branches of Government apply to activities on the base of Section 215 and Section 702. There is judicial oversight for activities that imply a capacity to compel information, including FISC orders for the collection under Section 215 and annual certifications that provide the basis for collection under Section 702. There is no judicial approval of individual selectors to query the data collected under Section 215 or tasked for collection under Section 702. The FISC operates *ex parte* and *in camera*. Its orders and opinions are classified, unless they are declassified. There is no judicial oversight of the collection of foreign intelligence outside the US under Executive Order 12333, which are conducted under the sole competence of the Executive Branch.

Annexes: Letters of Vice-President Viviane Reding, Commissioner for Justice, Fundamental Rights and Citizenship and Commissioner Cecilia Malmström, Commissioner for Home Affairs, to US counterparts

Ref. Ares(2013)1935546 - 10/06/2013

European Commission

Viviane REDING
Vice-President of the European Commission
Justice, Fundamental Rights and Citizenship

Rue de la Loi, 200
B-1049 Brussels
T. +32 2 298 16 00

Brussels, 10 June 2013

Dear Attorney General,

I have serious concerns about recent media reports that United States authorities are accessing and processing, on a large scale, the data of European Union citizens using major US online service providers. Programmes such as PRISM and the laws on the basis of which such programmes are authorised could have grave adverse consequences for the fundamental rights of EU citizens.

The respect for fundamental rights and the rule of law are the foundations of the EU-US relationship. This common understanding has been, and must remain, the basis of cooperation between us in the area of Justice.

This is why, at the Ministerial of June 2012, you and I reiterated our joint commitment to providing citizens of the EU and of the US with a high level of privacy protection. On my request, we also discussed the need for judicial remedies to be available to EU citizens when their data is processed in the US for law enforcement purposes.

It is in this spirit that I raised with you already last June the issue of the scope of US legislation such as the Patriot Act. It can lead to European companies being required to transfer data to the US in breach of EU and national law. I argued that the EU and the US have already agreed formal channels of cooperation, notably a Mutual Legal Assistance Agreement, for the exchange of data for the prevention and investigation of criminal activities. I must underline that these formal channels should be used to the greatest possible extent, while direct access of US law enforcement authorities to the data of EU citizens on servers of US companies should be excluded unless in clearly defined, exceptional and judicially reviewable situations.

Mr Eric H. Holder, Jr.
Attorney General of the United States Department of Justice
950 Pennsylvania Avenue, NW
Washington, DC 20530-0001
United States of America

[redacted]

Trust that the rule of law will be respected is also essential to the stability and growth of the digital economy, including transatlantic business. It is of paramount importance for individuals and companies alike. In this context, programmes such as PRISM can undermine the trust of EU citizens and companies in the Safe Harbour scheme which is currently under review in the EU legislative process.

Against this backdrop, I would request that you provide me with explanations and clarifications on the PRISM programme, other US programmes involving data collection and search, and laws under which such programmes may be authorised.

In particular:

1. *Are PRISM, similar programmes and laws under which such programmes may be authorised, aimed only at the data of citizens and residents of the United States, or also – or even primarily – at non-US nationals, including EU citizens?*

2. *(a) Is access to, collection of or other processing of data on the basis of the PRISM programme, other programmes involving data collection and search, and laws under which such programmes may be authorised, limited to specific and individual cases?*

   (b) If so, what are the criteria that are applied?

3. *On the basis of the PRISM programme, other programmes involving data collection and search, and laws under which such programmes may be authorised, is the data of individuals accessed, collected or processed in bulk (or on a very wide scale, without justification relating to specific individual cases), either regularly or occasionally?*

4. *(a) What is the scope of the PRISM programme, other programmes involving data collection and search, and laws under which such programmes may be authorised? Is the scope restricted to national security or foreign intelligence, or is the scope broader?*

   (b) How are concepts such as national security or foreign intelligence defined?

5. *What avenues, judicial or administrative, are available to companies in the US or the EU to challenge access to, collection of and processing of data under PRISM, similar programmes and laws under which such programmes may be authorised?*

6. *(a) What avenues, judicial or administrative, are available to EU citizens to be informed of whether they are affected by PRISM, similar programmes and laws under which such programmes may be authorised?*

   (b) How do these compare to the avenues available to US citizens and residents?

7. *(a) What avenues are available, judicial or administrative, to EU citizens or companies to challenge access to, collection of and processing of their personal data under PRISM, similar programmes and laws under which such programmes may be authorised?*

   (b) How do these compare to the avenues available to US citizens and residents?

Given the gravity of the situation and the serious concerns expressed in public opinion on this side of the Atlantic, you will understand that I will expect swift and concrete answers to these questions on Friday 14 June, when we meet at the EU-US Justice Ministerial. As you know, the European Commission is accountable before the European Parliament, which is likely to assess the overall trans-Atlantic relationship also in the light of your responses.

Yours sincerely,

ARES (2013) 2309322

VIVIANE REDING
VICE-PRESIDENT OF THE EUROPEAN COMMISSION
JUSTICE, FUNDAMENTAL RIGHTS AND CITIZENSHIP

CECILIA MALMSTRÖM
MEMBER OF THE EUROPEAN COMMISSION
HOME AFFAIRS

Brussels, 19 June 2013

Dear Secretary,

On Friday 14 June 2013 in Dublin we had a first discussion of programmes which appear to enable United States authorities to access and process, on a large scale, the personal data of European individuals. We reiterated our concerns about the consequences of these programmes for the fundamental rights of Europeans, while you gave initial indications regarding the situation under U.S. law.

At our meeting, you were not yet in a position to answer all the questions set out in the letter of 10 June 2013. Given the strength of feeling and public opinion on this side of the Atlantic, we should be grateful if you would communicate your answers to those questions as soon as possible. We are particularly concerned about the volume of data collected, the personal and material scope of the programmes and the extent of judicial oversight and redress available to Europeans.

In addition, we welcome your proposal to set up a high-level group of EU and U.S. data protection and security experts to discuss these issues further. On the EU side it will be chaired by the European Commission and include Member States' experts both from the field of data protection and security, including law enforcement and intelligence/anti-terrorism.

We suggest that we convene the initial meeting of this group in July. Our intention is to ensure that the European Commission will be in a position to report, on the basis of the findings of the group, to the European Parliament and to the Council of the EU in October.

We look forward to your reply.

Yours sincerely,

Viviane Reding

Cecilia Malmström

Secretary Janet Napolitano
Department of Homeland Security
U.S. Department of Homeland Security
Washington, D.C. 20528
United States of America

European Commission – rue de la Loi 200, B-1049 Brussels
eMail : Cecilia.Malmstrom@ec.europa.eu; Viviane.Reding@ec.europa.eu

ARES (2013) 2309328

VIVIANE REDING
VICE-PRESIDENT OF THE EUROPEAN COMMISSION
JUSTICE, FUNDAMENTAL RIGHTS AND CITIZENSHIP

CECILIA MALMSTRÖM
MEMBER OF THE EUROPEAN COMMISSION
HOME AFFAIRS

Brussels, 19 June 2013

Dear Attorney General,

On Friday 14 June 2013 in Dublin we had a first discussion of programmes which appear to enable United States authorities to access and process, on a large scale, the personal data of European individuals. We reiterated our concerns about the consequences of these programmes for the fundamental rights of Europeans, while you gave initial indications regarding the situation under U.S. law.

At our meeting, you were not yet in a position to answer all the questions set out in the letter of 10 June 2013. Given the strength of feeling and public opinion on this side of the Atlantic, we should be grateful if you would communicate your answers to those questions as soon as possible. We are particularly concerned about the volume of data collected, the personal and material scope of the programmes and the extent of judicial oversight and redress available to Europeans.

In addition, we welcome your proposal to set up a high-level group of EU and U.S. data protection and security experts to discuss these issues further. On the EU side it will be chaired by the European Commission and include Member States' experts both from the field of data protection and security, including law enforcement and intelligence/anti-terrorism.

We suggest that we convene the initial meeting of this group in July. Our intention is to ensure that the European Commission will be in a position to report, on the basis of the findings of the group, to the European Parliament and to the Council of the EU in October.

We look forward to your reply.

Yours sincerely,

Viviane Reding *Cecilia Malmström*

Mr Eric H. Holder, Jr.
Attorney General of the United States Department of Justice
950 Pennsylvania Avenue, NW
Washington, DC 20530-0001
United States of America

European Commission – rue de la Loi 200, B-1049 Brussels
eMail : Cecilia.Malmstrom@ec.europa.eu; Viviane.Reding@ec.europa.eu